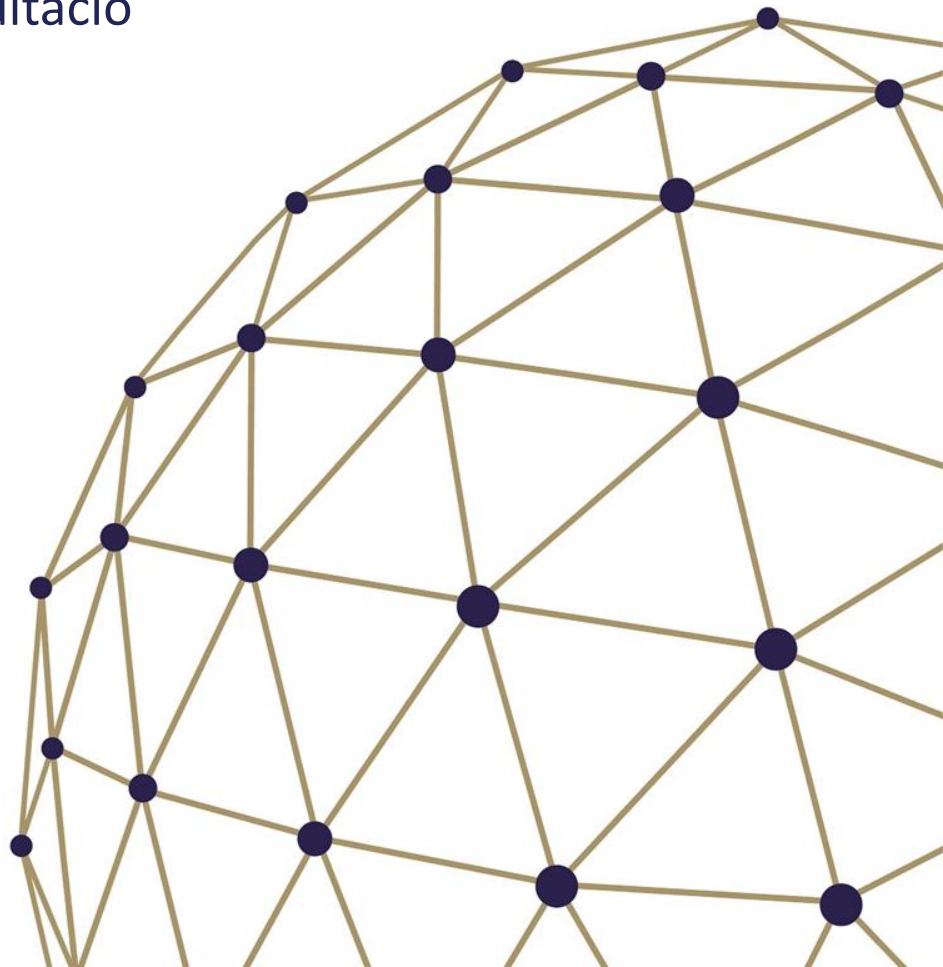
Informatikai felügyelet

Célok és módszerek

Biztosítási szakmai konzultáció

2016.12.19.

Gaidosch Tamás

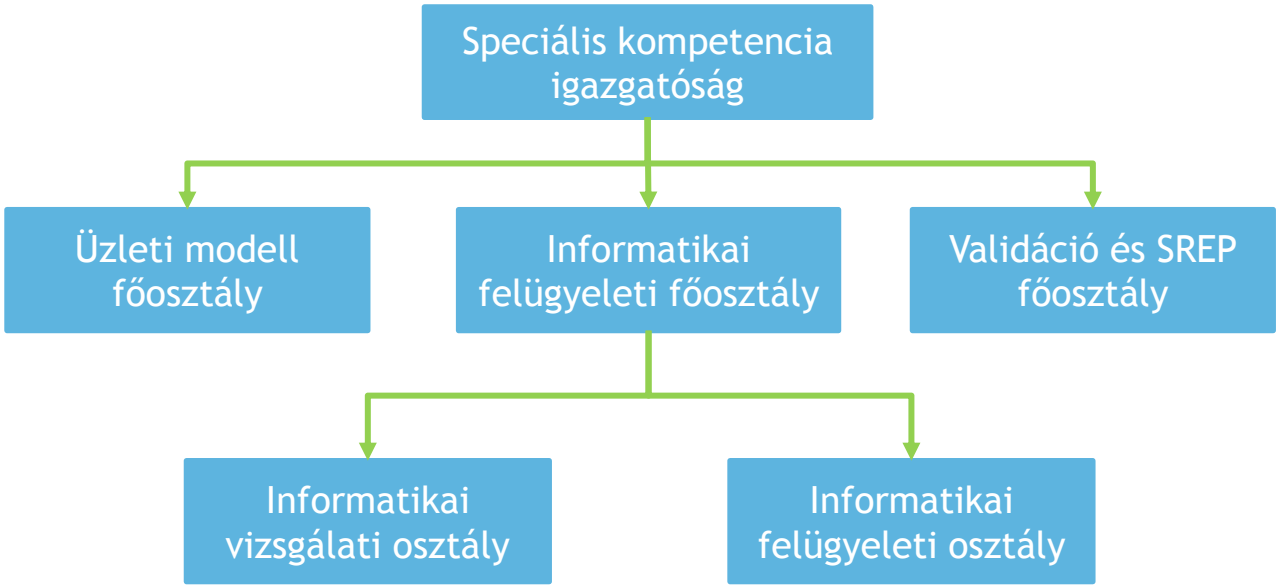


Tartalom

- Az Informatikai felügyelet
- Felügyeleti eszközök
- Gyakorlat és tapasztalat
- Hasznos tippek
- Kérdések

Az Informatikai felügyelet

- 2000-től működik
- Jelenleg főosztály
- Létszámkeret: 15 fő

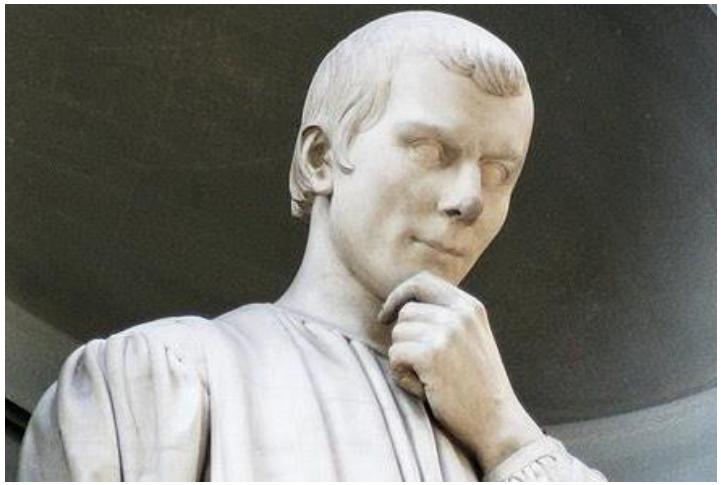


Az Informatikai felügyelet

- Célja: a felügyelt intézmények informatikai megfelelőségének biztosítása
- Mit jelent a „megfelelőség”?
  - Bit. (2014. évi LXXXVIII. törvény a biztosítási tevékenységről) és más ágazati törvények
  - 42/2015. Kormányrendelet a pénzügyi intézmények, a biztosítók és a viszontbiztosítók, továbbá a befektetési vállalkozások és az árutőzsdei szolgáltatók informatikai rendszerének védelméről
  - Az MNB1/2015. számú ajánlása az informatikai rendszer védelméről
  - Az MNB 15/2015. számú ajánlása az interneten keresztül nyújtott pénzügyi szolgáltatások biztonságáról
  - Szakmai standardok: ISO 27001, COBIT

Az IT prudens, megbízható és biztonságos működése

Prudens



„A cselekvés minden útja kockázatos, az elővigyázatosság tehát nem a veszély kerülésében rejlik (ami lehetetlen), hanem a kockázat kiszámításában és a határozott cselekvésben.”

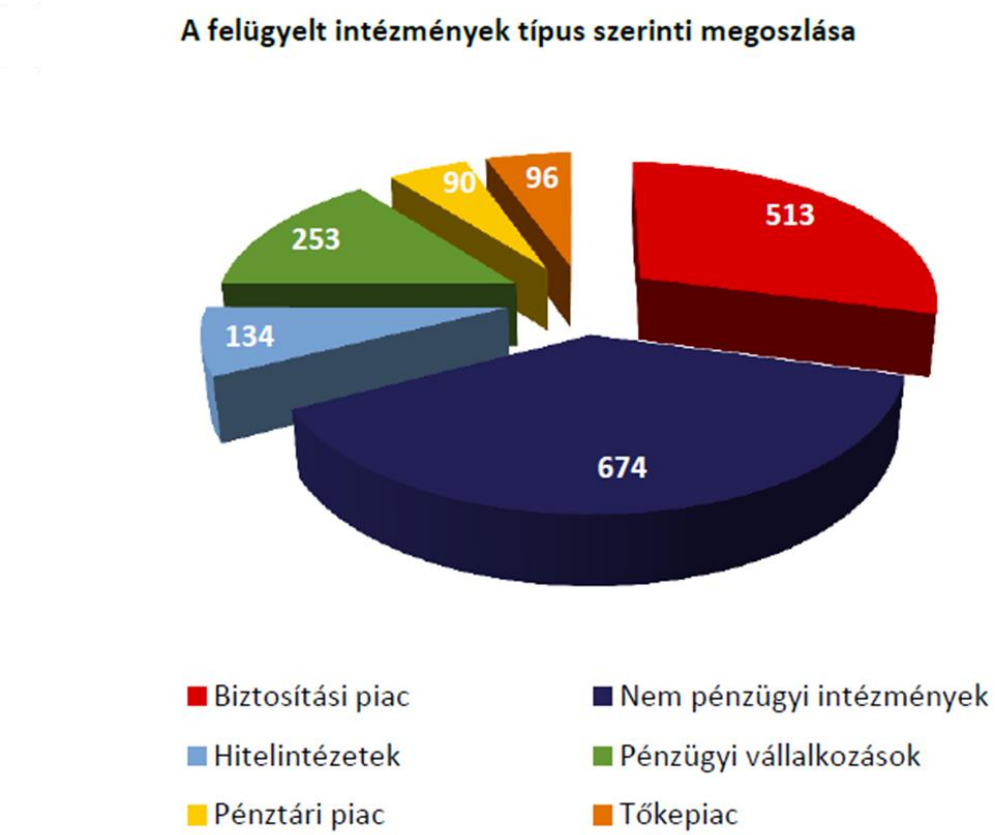
Niccolo Machiavelli

Biztonságos

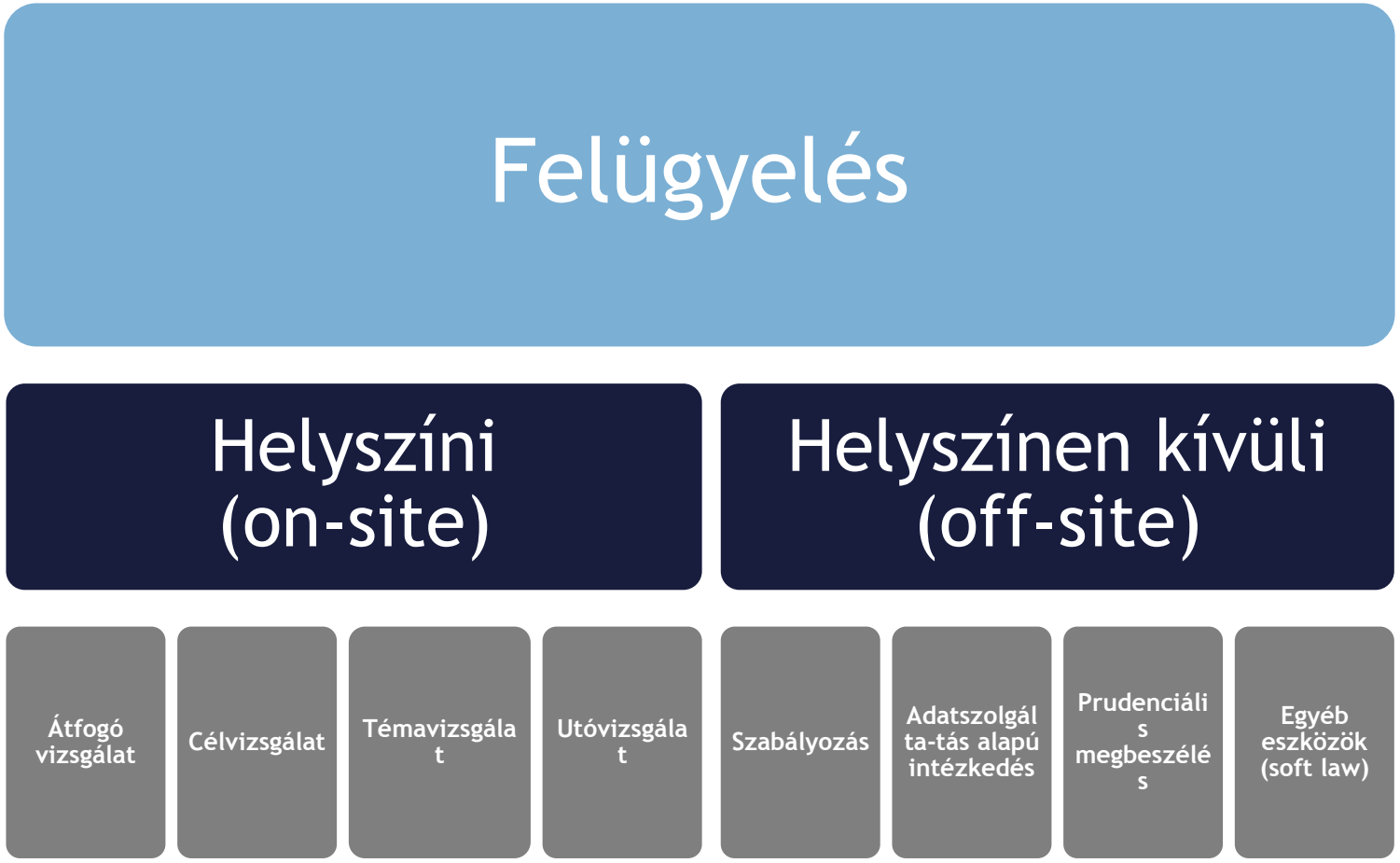
Stratégiai irányok

- Új területekre új módszerekkel
  - prudenciális szempontból nagyobb haszon
  - nagyobb bizonyosság
- Új kompetenciák fejlesztése / bevonása
  - adatelemzés
  - üzletifolyamat-elemzés
  - visszaélési kockázatok elemzése
- Soft law eszközök
- Együttműködés javítása
  - külső
  - belső

A felügyelt intézmények



Felügyeleti eszközök



Vizsgálatok

- Éves vizsgálati terv
- Ad-hoc vizsgálatok
- Módszertan
- Fókuszterületek

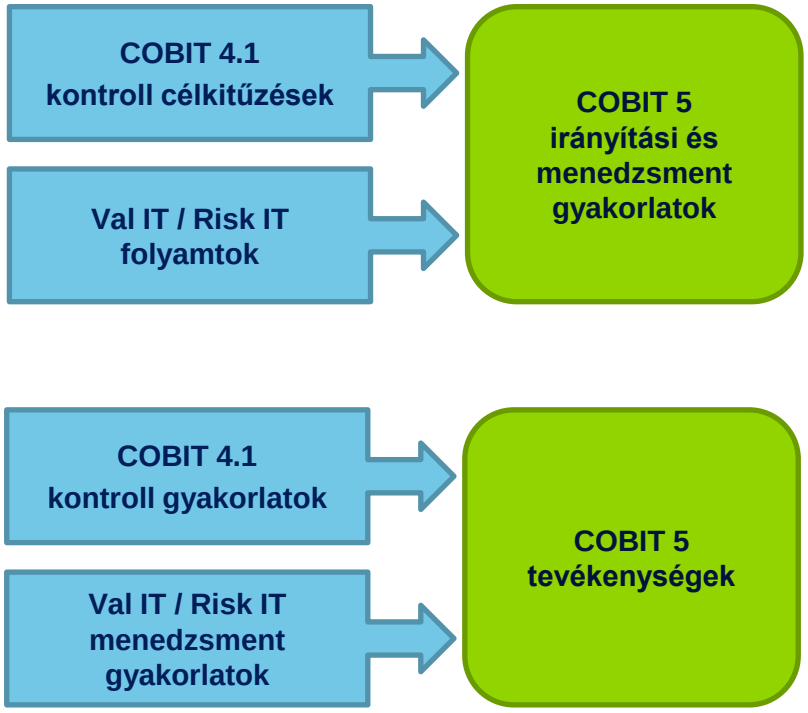
Módszertan

A Business Framework for the Governance and Management of Enterprise IT

COBIT: Control Objectives for IT

"We never got it right, in all these years, with the COBIT control objectives"

Eric Guldentops, 2011



Vizsgálati területek

- IT biztonsági vizsgálat
- Üzleti folyamatok IT támogatottságának vizsgálata*
- IT stratégiai vizsgálat*
- Visszaélési kockázatok vizsgálata*

- Általános IT kontrollok ellenőrzése
- Specifikus IT biztonsági kontrollok ellenőrzés

Mire keressük a választ?

Vizsgálat	Kérdés
IT biztonsági	Biztonságosan működik-e az IT? Jogszabályoknak megfelel-e az IT?
Üzleti folyamat támogatottsági	Alkalmazások jól kontrolláltak? Megbízhatunk-e a számokban? Adatok integritása biztosított?
IT stratégiai	Üzleti stratégia megvalósítható? CAPEX/OPEX reális? Nincs túl nagy kockázat a projektekben?
Csalás kockázati	Megfelelően csökkenti az IT a csalás kockázatát?

IT biztonsági vizsgálat: megközelítés

	Rendszer	Folyamat

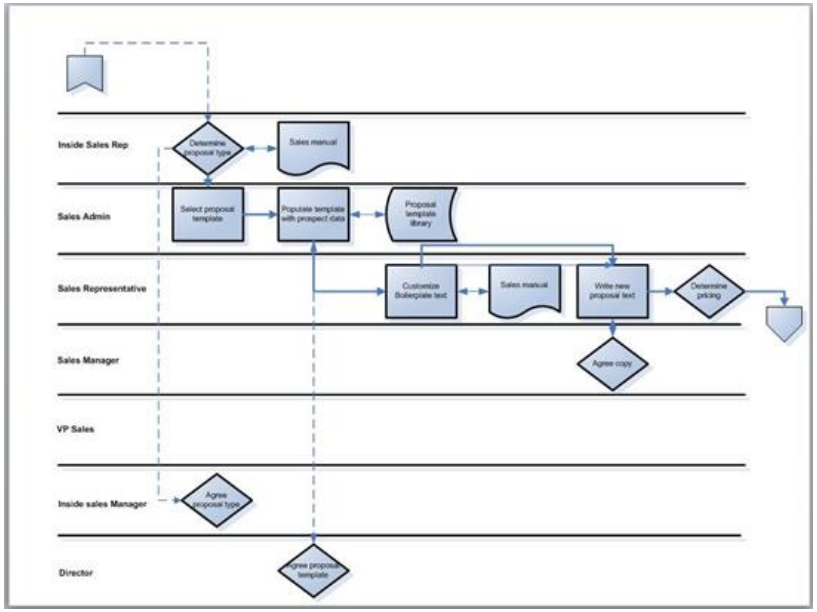
Magas kockázat	• Számla
	• Hitel
	• Értékpapír
	• Bankkártya
	• Elektronikus csatornák
	• Védelmi
	  ▪ tűzfalak, IDS/IPS
	  ▪ vírusvédelmi
	  ▪ adatszivárgás elleni
	  ▪ naplózó
	  ▪ központi jogosultságkezelő
		• Jogosultság-kezelés
		• Változáskezelés
		• BCP/DRP
		• Incidenskezelés
		• Kockázatkezelés
		• Fejlesztés
		• Stratégia
		• Projektvezetés
		• Naplóelemzés
		• Irányítás (Governance)

Közepes kockázat	• Számviteli • Távadatátviteli • Adattárház • Fióki (front-end)	• Program-menedzsment • Tesztelés • Beszerzés • Infrastruktúra-menedzsment • Archiválás

IT biztonsági vizsgálat: módszerek

- Dokumentáció vizsgálata
  - Rendben vannak-e a papírok?
  - Jogszabályi megfelelés dokumentáltsága
- Mintavétel és tesztelés folyamatok mentén
  - Tényleg úgy dolgoznak-e, ahogy lepapírozták?
  - Valójában jól dolgoznak-e?
- Konfigurációk vizsgálata
  - Biztonsági beállítások tételes vizsgálata

Üzleti folyamatok IT támogatottságának vizsgálata: módszer

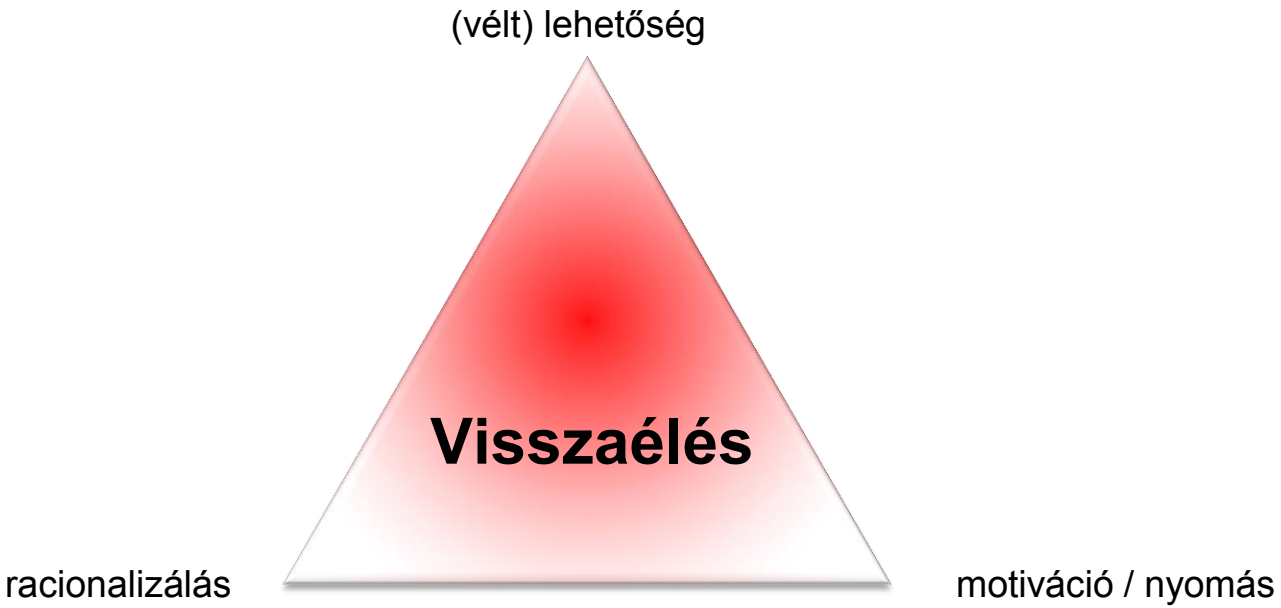


- Vizsgálandó folyamatok kockázat alapú kiválasztása
- Folyamat felmérése
- Közreműködő rendszerek azonosítása
- Adatáramlások felmérése (interfészek)
- Kontrollok azonosítása és értékelése
  - Alkalmazás szintű kontrollok
  - Interfész kontrollok
  - Szubsztantív eljárások (opcionális)
- Dokumentáció és következtetés

IT stratégiai vizsgálat: módszer

- Üzleti stratégiai célok megismerése
- IT stratégiai célok megismerése
- Korreláció
- Projekt portfolió áttekintése
  - Magas kockázatú projektek azonosítása
- CAPEX/OPEX tervek értékelése
- Dokumentáció és következtetés

Visszaélési kockázatok vizsgálata: megközelítés

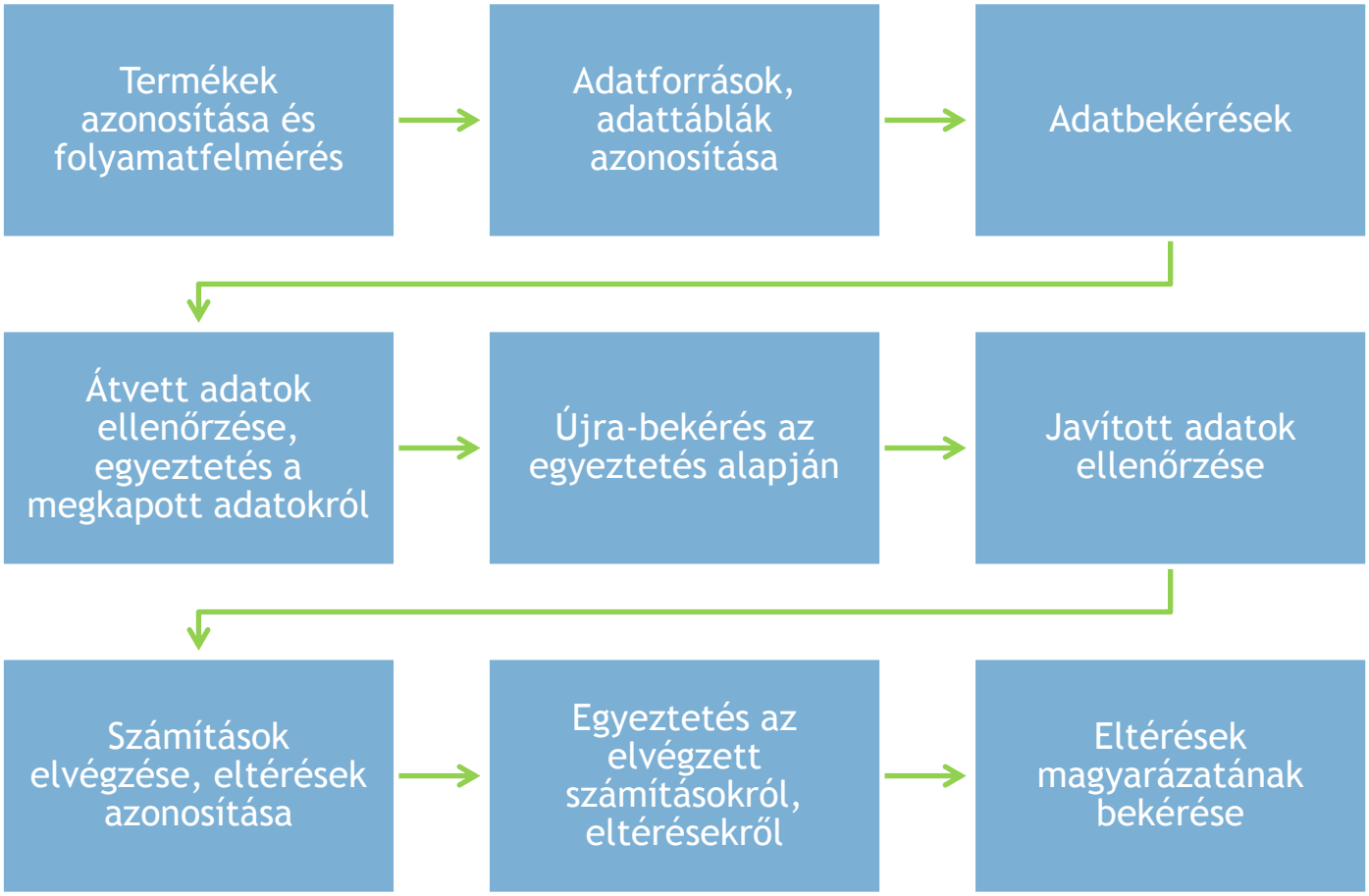


Visszaélés háromszög (Fraud Triangle)

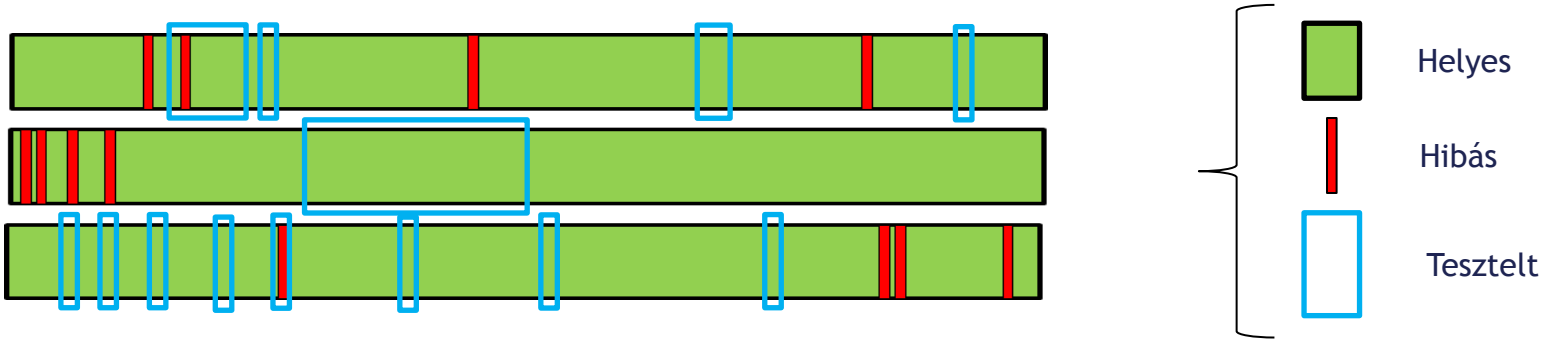
Visszaélési kockázatok vizsgálata: módszer

- Magas kockázatú alkalmazások/funkciók azonosítása
- Jogosultságok vizsgálata
- Naplózás vizsgálata
- Gyanús tranzakciók keresése
  - Adatelemzés
- Dokumentáció és következtetés

Adatelemzés



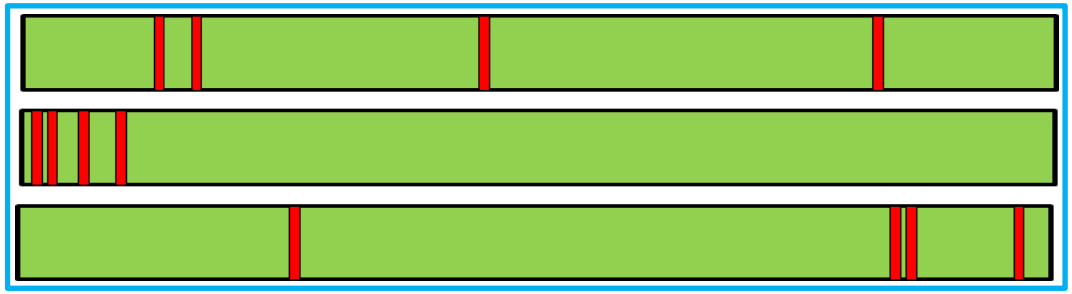
Mintavételes tesztelés

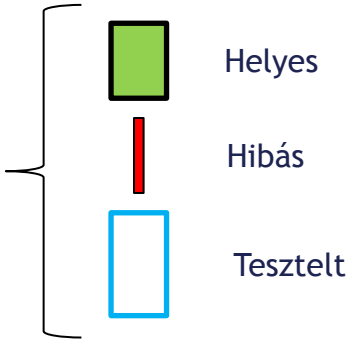


Problémák

- Mekkora legyen a minta?
- Mi legyen a mintavétel módszere?
- Milyen eséllyel találunk hibás tételt?
- Mit tegyünk, ha hibás tételt találtunk?
- Mit tegyünk, ha visszaélésre gyanakszunk?

Teljes populációs tesztelés





Problémák

- Ki ért hozzá?
- Mekkora lesz a ráfordítás?
- Hogyan automatizáljuk?

Összehasonlítás

Mintavétel	Teljes populáció
Kockázatértékelés szükséges	Kockázatértékelés nem szükséges (máshol szükséges)
Bizonyosság a mintaméret függvénye	Maximális bizonyosság
A mintavétel nem mindig szakszerű (az eredmény félrevezető lehet)	Nem merül fel a probléma
Nem egyértelmű teendők gyanús tételek esetén	Egyértelmű teendők gyanús tételek esetén
Könnyebb végrehajtani	Nehéz végrehajtani
Kézi módszerek alkalmazhatók	Kézi módszerek ritkán alkalmazhatók

Milyen vizsgálatokat nem végzünk?

- Titkos vizsgálatok
- Hacker eszközökkel végzett vizsgálatok
  - Vulnerability scan
  - Exploitation
- IT visszaélés-felderítési vizsgálatok

Tipikus problémák

- Jogosultságkezelés gyengeségei
- Naplóelemzés alacsony hatásossága
- DRP (katasztrófahelyzet) felkészülés hiányosságai
- Kockázatelemzés hiányosságai
- Kiszervezéssel kapcsolatos félreértések

„Feltörekvő” problémák

- Felhőbe való kiszervezés
- Shadow IT
- MDM (mobileszköz-menedzsment) hiánya
- Erőforráshiány

Hasznos tippek a felügyeleti vizsgálathoz

- Felkészülés
  - Ne gyártsunk fiktív vagy irreleváns dokumentumokat
  - A „nincs ilyen” nem feltétlenül rossz válasz
- Helyszíni szakasz
  - Tartsuk a menetrendet (interjúk és adatkérések)
  - Küldjünk releváns és felkészült kollégákat az interjúkra
  - Ne beszéljünk mellé és főleg ne akadályozzunk
  - Érdemes érvelni, visszakérdezni, pontosítást kérni
  - Biztosítsuk a technikai feltételeket
- Jelentés
  - Záró megbeszélés fontossága
  - Érdemes a véleményezési lehetőséget kihasználni, tévedésekre rávilágítani, hiányzó bizonyítékokat pótolni

Összefoglalva

- Az IT Felügyelet a felügyelt intézmények informatikájának prudens, megbízható és biztonságos működését támogatja és ellenőrzi
- Hangsúlyos az IT biztonság vizsgálata (jogszabály alapján)
- Új területeket is vizsgálunk: üzleti folyamatok IT támogatottsága, IT stratégia, visszaélés kockázata
- Adatelemzés
- Nem hekkerkedünk
- Nem nyomozunk

Köszönöm a figyelmet!